

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



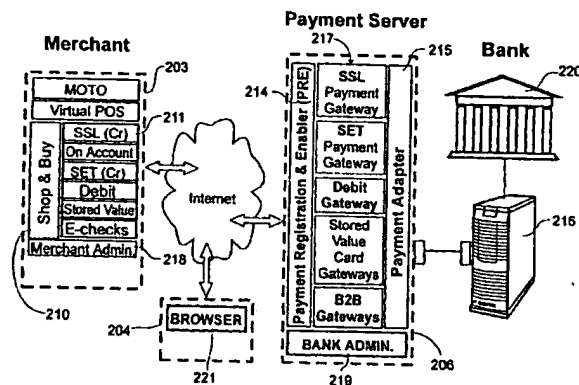
(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80100 A1

- (51) International Patent Classification⁷: G06F 17/60
- (21) International Application Number: PCT/AU01/00430
- (22) International Filing Date: 17 April 2001 (17.04.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
PQ 6965 17 April 2000 (17.04.2000) AU
- (71) Applicant (for all designated States except US): QSI PAYMENT TECHNOLOGIES PTY LTD [AU/AU]; Level 22, 300 Adelaide Street, Brisbane, QLD 4000 (AU).
- (74) Agent: FISHER ADAMS KELLY; Level 13, AMP Place, 10 Eagle Street, Brisbane, QLD 4000 (AU).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): LYTHALL, Colin, Victor [AU/AU]; 4 Avebury Street, Hill End, QLD 4101 (AU). CHALKER, Dean, Andrew [AU/AU]; 18 Vera Street, Toowong, QLD 4066 (AU).
- Published:
— with international search report
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ELECTRONIC COMMERCE PAYMENT SYSTEM



WO 01/80100 A1

(57) Abstract: A payment method and apparatus for electronic commerce involving a payer or customer computer (204), a payee or merchant computer (203) and at least one payment gateway (217) on a payment server (206). In operation, the payee computer creates, in response to transmission of a payment request from the payer computer over a communications link (212) to said payee computer, a transaction order containing a transaction amount, a transaction identifier and a payee identifier. The payee computer (203) transmits the transaction order to the payment gateway over a secure communications link, and links the payer computer to the relevant payment gateway. The payment gateway validates the transaction order, obtains payment details associated with the transaction request from the payer computer, and forwards the transaction amount and payment details to a financial network (216, 209) for further processing. The payment gateway produces a transaction receipt in response to said further processing by the financial network, transmits the receipt to the payee computer (203), and re-links the payer (204) computer to the payee computer. The payee computer (203) transmits transaction status information contained in the transaction receipt to the payer computer (204). Suitably both the transaction order and the transaction receipt are digitally signed and encrypted in order to facilitate authentication of the transmitting party and to protect the integrity of the respective contents of the transaction order and receipt.

TITLE OF THE INVENTION
"ELECTRONIC COMMERCE PAYMENT SYSTEM"

BACKGROUND OF THE INVENTION

5 (I) Field of the Invention

This invention relates to a computerised system for facilitating financial transactions in electronic commerce. The invention particularly, although not exclusively, relates to a method and apparatus for conducting secure electronic payments via a public communications network involving customers, merchants and their financial
10 institutions.

(II) Discussion of the Background Art

Present systems for facilitating electronic commerce employ, at least in part, the global communications network known as the Internet. The uptake of electronic
15 commerce is considered, in some quarters, to be constrained by customer concerns about the security measures available for protecting both their personal details and details of their financial instruments, most notably bank account and card details. This is a concern for both businesses who are customers for the goods and services of other business merchants and for private individual customers. Recent media reports of unauthorised
20 access to details of financial instruments held in databases maintained by high profile corporations, continue to fuel such concerns.

Some financial institutions have been quick to recognise the potential for electronic commerce to reduce overheads and streamline business processes. However, significant banking and business accounting resources continue to be expended in the
25 daily handling and processing of paper cheques. Financial institutions have over-riding concerns about the strength of available security measures for electronic commerce together with the cost of servicing a proliferating range of security protocols and payment schemes. Examples include magnetic stripe systems, smart card based systems, electronic purse systems and digital cash for use in credit, debit and/or stored value
30 modes.

US Patent No. 5850446 assigned to Verifone, Inc. describes a system for virtual point of sale processing utilising an extensible, flexible architecture. The system uses secure electronic transaction (SET) messages and extensions to the SET message protocol to transmit payment information between a merchant computer system and a

payment gateway computer system. The SET protocol requires the use of digital certificates to authenticate merchants to the payment gateway and vice versa. However, digital certificates are expensive and must be installed in the SET software executing on the merchant computer system which is not necessarily a simple task. Digital certificates are generally of a limited duration, require renewal prior to expiry and are not in widespread use. Furthermore, digital certificates require the intervention of a trusted third party with attendant administrative and logistical overheads relating to certification maintenance and revocation. The trusted third party is then able to vouch for two parties who are otherwise not known to one another.

The proprietary extensions proposed to the SET protocol in the Verifone patent necessarily deviate from the SET standard. When the extensions are used, they would not receive brand certification as standard SET transactions as required within a banking system for the purposes of inter-operability, non-repudiation or transaction risk analysis. This typically results in an increased fee structure charged to the merchant. The standard SET protocol is unable to handle transactions using debit or smart card protocols, and is limited to a credit card transaction. The Verifone system also requires the installation of a network interface processor at each of the payment gateway systems and at each financial institution. This requirement adds further cost to system installation and operation.

A further problem with conventional electronic commerce systems is that customer financial details are generally exposed to the merchant. Whilst it is true that the SET protocol provides a wallet mechanism which secures this information, the reality is that very few customers have their own digital certificate as necessary to implement the SET wallet.

BRIEF SUMMARY OF THE INVENTION

(I) Object of the Invention

It is an object of the present invention to provide an electronic commerce payment system that ameliorates or overcomes at least some of the problems associated with the prior art.

It is another object of the present invention to provide a method of conducting electronic transactions that addresses security concerns of customers (payers), whilst offering commercial organisations (payees) savings in financial and business resources.

It is yet another object of the present invention to provide an apparatus for conducting electronic transactions that supports a wide range of payment systems and is sufficiently flexible allowing extensions to proposed payment systems.

5 It is a still another object of the present invention to provide an electronic commerce payment system wherein payers, payees and participating financial institutions may be assured of the security of communications, including both the integrity of transmitted data and the authenticity of a party originating the data.

Further objects will be evident from the following description.

10 (II) Disclosure of the Invention

In one form, the invention resides in a payment method for electronic commerce involving a payer computer, a payee computer and a payment gateway, said method including the steps of:

15 (a) the payee computer creating, in response to transmission of a payment request from the payer computer over a communications link to said payee computer, a transaction order containing a transaction amount, a transaction identifier and a payee identifier;

20 (b) the payee computer transmitting the transaction order to the payment gateway over a secure communications link, and linking the payer computer to the payment gateway;

(c) the payment gateway validating the transaction order, obtaining payment details associated with the transaction request from the payer computer, and forwarding the transaction amount and payment details to a financial network for further processing;

25 (d) the payment gateway producing a transaction receipt in response to said further processing by the financial network, transmitting the receipt to the payee computer, and re-linking the payer computer to the payee computer; and

(e) the payee computer transmitting transaction status information contained in the transaction receipt to the payer computer.

30 Suitably both the transaction order and the transaction receipt are digitally signed and encrypted in order to facilitate authentication of the transmitting party and to protect the integrity of the respective contents of the transaction order and receipt.

Preferably the transaction request from the payer computer is transmitted over a secure communications link.

The transaction request may include the transaction amount and a transaction identifier.

If required, the transaction request may contain details of items to be purchased.

Suitably the processing by the financial network involves authorisation of payment and occurs in real time.

In a further form, the invention resides in a payment apparatus for effecting payment transactions in electronic commerce, said payment apparatus including:

(a) a payee computer operative to receive a transaction request from a payer computer over a communications link and creating, in response to the transaction request, a transaction order containing a transaction amount, a transaction identifier and a payee identifier;

(b) the payee computer also operative to transmit the transaction order to a payment gateway over a secure communications link, and to effect linking of the payer computer to a payment gateway;

(c) the payment gateway operative, subsequent to validating the transaction order, to obtain payment details associated with the transaction request from the payer computer and to forward the transaction amount and payment details to a financial network for further processing;

(d) the payment gateway also operative to produce a transaction receipt in response to said further processing by the financial network, to transmit the receipt to the payee computer, and to effect re-linking of the payer computer to the payee computer; and

(e) the payee computer then operative to transmit transaction status information contained in the transaction receipt to the payer computer.

Preferably a payment client application is resident on the payee computer to facilitate secure communications with the payment gateway.

The payment gateway is suitably one of a plurality of such gateways hosted on a payment server, which payment server also hosts a payment registration enabler application and a payment adapter application.

In preference the payment registration enabler application generates unique identifiers for payment clients registered with the payment server.

In preference the payment adapter application provides an interface between the respective gateways and financial networks.

5 In a still further form the invention resides in a method of conducting electronic transactions involving a customer for goods or services supplied by a merchant, wherein a customer browser and a merchant server can communicate with each other and with a payment server and the payment server can communicate separately with a plurality of financial institutions, said method including the steps of:

10 (a) the customer browser transmitting a payment request for one or more items desired to be purchased by the customer to the merchant server;

(b) the merchant server providing a merchant identifier, transmitting the merchant identifier together with a session identifier and payment amount required for the desired items over a secure communications link to the payment server, and redirecting the customer browser to the payment server;

15 (c) the payment server validating the merchant identifier and requesting payment information from the customer, then using the session identifier and payment details to seek approval for payment from the customer's financial institution;

(d) the payment server providing a receipt to the merchant server regarding the approval over the secure communications link and redirecting the customer browser
20 to the merchant server;

(e) the merchant server providing approval status information about the transaction for purchase of the items to the customer browser.

Suitably step (a) involves the customer perusing electronic catalogues and adding items of goods or services to a virtual shopping basket application executing on the
25 merchant server in order to identify the desired items.

In step (a), delivery information obtained from the customer may also be transmitted to the merchant server.

Preferably in step (b), the merchant server executes a payment client application that creates a digital order containing the merchant identifier, session identifier and
30 payment amount, which digital order is transmitted to the payment server.

Preferably in step (c) the payment information includes payment method and payment detail.

The digital order may further contain a locale identifier denoting the language to be used in presentations to the customer by the payment server and a return universal

resource locator (URL) which enables the payment server to route a digital receipt to the merchant server or associated merchant application, eg. an ERP system.

Most preferably the digital order is secured and authenticable by means of a merchant key pair recognisable by the payment server.

5 If required, security for the digital order includes encryption of the information contained along with a digital signature to effect authentication and message integrity.

In a yet further form, the invention resides in an electronic transaction apparatus for use in conjunction with a merchant server hosting a shop & buy application allowing
10 a customer to peruse, via a communications link with a customer computer, goods and services supplied by the merchant, said apparatus including:

(a) a plurality of payment clients for integration with the shop and buy application on the merchant server, said payment clients facilitating secure communications with a payment server using respective payment protocols;

15 (b) a payment server having a plurality of payment gateways corresponding to at least one of the payment clients of the merchant server and a payment adapter providing an interface for separate communications with a plurality of financial institutions;

(d) the payment server operative to process customer payment orders
20 produced by a payment client in response to the shop and buy application and transmitted by the merchant server;

whereby, in use:

(i) the customer computer is redirected to the payment server to
25 obtain payment details from said customer in order to seek approval from the customer's financial institution, and

(ii) the payment server provides a receipt to the merchant server regarding the approval and redirects the customer computer back to the merchant server.

30 Preferably the shop and buy application is an Internet shopfront accessible by a browser application resident on the customer computer.

The payment clients are suitably implemented using active code for execution by a virtual machine emulator resident on the merchant server.

Suitably the payment server provides a secure communications link between the payment server and the customer.

In one form the secure communications link may employ secure sockets layer (SSL) technology.

The customer order is preferably a digital order containing a merchant identifier, a session identifier and a payment amount required by the merchant for items desired by the customer.

Preferably the payment server includes a transaction database for recording details of payment transactions for merchants.

The merchant receipt is preferably a digital receipt containing an authorisation code for the customer.

The redirection of the customer computer back to the merchant server may occur before or simultaneously with provision of the merchant receipt.

Suitably the payment server further includes a payment registration application that generates and distributes pairs of security keys to respective payment clients.

Preferably both the digital order and the digital receipt are encrypted and digitally signed, when required, using the security key pairs.

BRIEF DESCRIPTION OF THE DRAWINGS

To assist in understanding the invention preferred embodiments will now be described with reference to the following figures in which:

FIG. 1 is an illustration of a prior art electronic commerce payment system;

FIG. 2 is an illustration of a first embodiment of an electronic commerce payment system in accordance with the present invention;

FIG. 3 is an illustration of the components of the payment server and associated payment client application;

FIG. 4 is a process flow diagram for a preferred method of conducting a secure three party financial transaction;

FIG. 5 is an illustration of a second embodiment of an electronic commerce payment system in accordance with the present invention; and

FIG. 6 is an illustration of a system for conducting an n-party transaction relating to the second embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The prior art arrangement illustrated in FIG 1 includes a merchant site 101 having an enterprise resource planning (ERP) computer system 102 and a shop & buy computer system 103. The merchant ERP system typically hosts ERP and/or accounting applications that communicate with a merchant shop & buy application. The shop & buy system 103 hosts the shop & buy application that facilitates browsing of goods and services offered to customers via a public communications network, such as the Internet. It will be appreciated that the merchant shop & buy application may be hosted at the merchant site 101, as in the present arrangement, or at a remote site by an Internet service provider (ISP) or commerce server provider (CSP). One particular example of a central CSP arrangement, which is not necessarily typical, is described in International Patent Publication No. WO 99/07121 in the name of NetAdvantage Corporation.

The shop & buy system 103 is thus periodically in communications with a customer or "payer" system 104 at a payer site 105 via the Internet. Conventionally, when a customer has identified items desired to be purchased from the merchant, details of the customer's preferred payment instrument are also obtained from the customer. The customer's payment details are typically stored in the merchant's shop & buy system 103 and also transmitted to a payment server computer 106, associated with the payment instrument, for authorisation. Unless the customer has a SET wallet (or similar) mechanism, the customer's financial details are exposed to the merchant. The exposure of client financial details greatly heightens the risk of fraud, either by unauthorised access to the shop & buy system 103 or by the merchant's employees.

The authorisation process may involve a third party trusted authority 107 to verify the identity of both the merchant and the payer, as required. In many cases the payment server 106 is maintained by a credit card association, such as American ExpressTM, MasterCardTM or VisaTM. The payment server 106 obtains credit authorisation for the payment tendered by the customer from the payer bank computer system 108. In some circumstances, the payee bank 109 may also arrange for the payment to be credited to the merchant's trading account. Thus it will be appreciated that the prior art transaction process is a complex distributed procedure, wherein the merchant computer systems are involved in unnecessary detail which is accordingly error prone.

An electronic commerce payment system of a first embodiment of the invention will be described in relation to FIGS. 2 and 3 of the drawings. It should be appreciated that, in some contexts, the term "payment" will contemplate mere authorisation, or even

reversal, of a funds transfer process. The merchant site 201 includes payee computers such as a merchant ERP computer system 202 and a merchant shop & buy computer system 203. The shop & buy computer system 203 hosts a shop & buy application 210, such as an Internet store-front, and a payment client 211. When coupled by a communications link 212, the shop & buy application 210 allows customers to peruse electronic catalogues of goods and services available from the merchant. The customer uses a browser application 221, such as a generic Internet browser, resident on the customer (or payer) computer system 204 at the customer site 205. An Internet browser that supports server-gated cryptography (SGC), such as version 4 or higher of Microsoft Corporation's Internet Explorer™ or Netscape's Navigator™, allowing 128 bit secure SSL sessions is preferred. Security aspects of communications links using Internet for transport purposes are discussed in further detail below.

The payment client 211 is suitably a platform independent software component, preferably of "thin client" type, that facilitates secure communication with the payment server 206. The payment client 211 is implemented using an active code, such as the Java™ language, to facilitate portability and ease of integration with a wide range of merchant shop & buy applications written in a variety of programming languages. The payment client provides for a wide range of transaction protocols and enabling technologies in addition to the secure sockets layer (SSL) interface suited to the customer using an Internet browser application, including:

- multiple payers to single payee transactions eg. mail order, telephone order (MOTO) protocols;
- virtual point-of sale (POS) protocols for credit or debit;
- on-account arrangements;
- secure electronic transaction (SET) for credit cards;
- debit arrangements;
- stored value (smart) cards, eg. Mondex and VisaCash;
- purchasing cards; and
- electronic checks.

The payment server 206 hosts a number of applications, including a payment registration enabler (PRE) application 214 and a payment adapter 215. The PRE application 214 performs the role of generating unique identifiers for the payment clients of each registered user (payer or payee), through the creation of unique cryptographic key pairs embedded in the enabling software. Thus the PRE provides an automated

Internet based means to centrally register payers or payees and to distribute enabling technology, typically to customers of financial institutions such as banks 220.

The payment adapter 215 provides the interface to the appropriate financial networks, such as the customer/payer bank computer system 208 and the merchant/payee bank computer system 209. The payment adapter 215 communicates with financial institution host computer systems using the standard real-time messaging protocols used by the institutions, such as the ISO 8583 or AS 2805 protocols. If required the embodiment can further include implementation of an ISO8583/AS2805 front-end processor/switch 216. This allows multiple connections to host systems, either in the same bank 220 or to other financial institutions or card associations.

The payment server 206 also hosts a series of payment gateways 217 that provide specific functionality for particular payments or transaction protocols, such as one or more of SSL, SET, debit, stored value and business to business (B2B) gateways. The payment server database (not illustrated in FIG. 3) contains full merchant configuration and transactional records. Statistical information may be maintained for each merchant on a daily, weekly and monthly basis. Similarly, statistical records are also maintained for each gateway. The merchant administration interface 218, provided to the merchant via browser access, provides a window for merchants to securely administer their Internet originated financial transactions. Administration functions include payment captures, reversals or credits, reconciliations and historical transaction searches. Access to merchant administration information is also available to the merchant application through the payment client interface 210. Reporting capabilities include transaction type breakdown, trend analysis and receipt of bank statements and advices.

The bank administration interface 219, provided at the payment server 206, provides a window for banks 220 to securely administer the merchant relationship and for merchant service support. Administration functions include merchant set-up, revocation, merchant profile definition, instrument registration and security.

Merchants wishing to use electronic commerce systems require on-line real-time authorisations for financial transactions, particularly those involving credit cards or smart cards. The payment client 211 of the present embodiment provides merchants with a secure on-line transaction link from a cardholder directly into the merchant's bank computer system 209. The payment client 211 provides an interface between the merchant shop & buy application 210 and the applications hosted by the payment server 206 which facilitate access to financial institutions. In brief the payment client includes

several application program interfaces (APIs) for use by the shop & buy application. The embodiment of the invention will be further described with reference to a typical 3-party customer (payer) to merchant (payee) financial transaction.

When a customer identifies, using the Internet browser, one or more items desired
5 to be purchased and places them into a virtual shopping basket provided by the shop & buy application 210. The shop & buy application 210 uses the payment client 211 to create a digital order (DO), in response to the customer's request to make payment at a virtual check-out. The digital order passes information, including a merchant identifier, a session identifier and a total order amount, to the payment server 206 and the payment
10 client re-directs the customer browser to the payment server 206. The payment server (not the merchant) will then prompt the customer to select a desired payment protocol (such as SSL+ or SET) and payment instrument (such as American Express, MasterCard or Visa) from those available. The payment server then follows with a request for specific details of the payment instrument, ie. credit card number and expiry date, to be
15 provided by the customer.

The payment server 206 then uses the information from the digital order and the payment details obtained directly from the customer to prepare suitable financial transactions, and switch 216 these transactions to an appropriate financial network 208, 209. On receipt of a corresponding transaction result message (such as "transaction
20 approved") from the financial network, the payment server 206 will create a digital receipt (DR). The digital receipt is transmitted to the merchant server and the customer's browser is re-directed back to the shop & buy application 210 hosted on the merchant computer system 203.

The redirections to and from the customer browser application are done via a
25 HTTP or HTTPS protocol "redirect" or "meta-refresh" operation, which minimises any redirection warning messages from the browser. The digital order and digital receipt messages between the merchant's shop & buy application 210 and the payment server 206 are effectively "carried" by the browser hosted on the customer's computer system 204. The customer's TCP/IP connection is switched between the merchant computer
30 system 203 and the payment server 206. During the payment process, the customer is connected to the payment server 206 and the merchant cannot gain access to payment details. The DO and DR messages are digitally signed and encrypted in addition to the intrinsic cryptographic security of the SSL session. In another embodiment 280-bit encryption is proposed, but other key lengths can also be supported.

Asymmetric key cryptography (using public and private keys generated by the owner of the payment server) is used to secure communication between the payment client 211 and the payment server. The payment client encrypts messages with the payment server public key; the payment server de-crypts messages with the payment server private key. This arrangement seeks to ensure message content privacy. A corresponding approach is used to ensure privacy of messages travelling in the other direction. Transaction authenticity and integrity protecting against malicious tampering or communication errors is achieved via signing (prior to encrypting) the transaction with the sender's private key; the signature is verified using the sender's public key.

The operator of the payment server controls the generation and distribution of the payment client keys, which overcomes some of the more general PKI issues. Payment client keys are generated by the payment server, and integrated into the payment client. There is a "tight" relationship between an individual payment client and associated payment server - payment clients cannot connect to an alternative payment server at will. The keys are suitably stored in highly encrypted form on the payment server. Tamper-resistant hardware security modules (HSMs) are used by the payment servers to store the sets of master and working keys used to encrypt and decrypt payment client keys. The master and working keys are not exportable from the HSMs. The HSMs also generate the payment client keys.

The payment server uses Server-Gated Cryptography (SGC) to enhance US-export grade browsers SSL session strength to 128-bit. SGC is supported by version 4 and higher browsers, although the "export" versions of such browsers otherwise support only 40-bit SSL sessions. The Payment Server uses a standard "web server" to serve the payment screens to the client browser. The Payment Server retains session and state information via an electronic token known as a "cookie", stored transparently in the customer's browser if enabled. Otherwise a hidden HTML field is used. This facilitates the linking of the digital order and payment details within a corresponding digital receipt (DR). The financial transaction and switching process can be quite complex, consider for example:

- a credit card transaction may be routed to the merchant's (acquiring) bank;
- the acquiring bank may then seek authorization from the customer's (issuing) bank; and

- the issuing bank may decline the transaction, or issue an authorization number (which lessens the cardholder's available credit, but does not actually place a charge).

5 In this example the authorized funds would be "captured" (in full, or in part) via a subsequent transaction – perhaps as part of a picking and shipping process.

In order to understand the financial transaction method of the invention, a preferred method is described with reference to FIG. 4 of the drawings. The steps in the transaction method, which involve a merchant server 401, a customer browser 402 and a payment server 403, are as follows:

- 10 (1) The customer (payer) browses an electronic catalogue of the merchant's goods and services, via a shop & buy application hosted on the merchant (payee) server 401. Identified items are added to a virtual shopping trolley by the customer.
- 15 (2) When the customer elects to "check out" and make payment for items in the virtual shopping trolley, the merchant server 401 processes those items. Where appropriate, delivery details are also sought from the customer by the shop & buy application.
- 20 (3) The shop & buy application uses the payment client to generate a digital order (DO) which is then sent to the payment server 403. The digital order contains a merchant identifier, a session identifier, the payment amount, the locale and optionally a return URL. The digital order is digitally signed using the site key and encrypted using the public payment server key. An encrypted digital order message is transmitted to the payment server as an HTTP re-direction through the
25 customer's browser. The customer is transferred transparently to the payment server.
- 30 (4) The payment server 403 performs a database look-up to retrieve the public key of the merchant and the registered digital signature. This allows the payment server to validate the digital order by decrypting the digital order message to check the digital signature contained in the digital order. The payment server then presents to the customer a list of payment protocol and payment instrument options (eg. 3-party authenticated SSL and Visa credit card), as supported by the merchant's acquiring bank and payment server proprietor.

- (5) The customer selects their preferred payment method, ie. protocol and instrument, from those presented by the payment server.
- 5 (6) The payment server 403 presents an input screen via the browser, prompting the customer for details required for the selected payment protocol and instrument, eg. credit card number and expiry date. Some payment protocols may require the customer to use a token (such as a smart card) along with a secret (such as a pass word or PIN) to authenticate themselves to the payment server or to a specific
10 financial institution.
- (7) The customer enters the required details, which are edit checked by the payment server, eg. for invalid credit card number. In the case of a token, the customer or payee may be required to down-load an active software component (for example a
15 Java applet) to enable a secure connection to be established between the token reader (eg. smart card reader) and the payment server. This active component is controlled and served from the appropriate gateway of the payment server.
- (8) The payment server 403 communicates with financial networks 404 - which
20 generally include separate, dedicated and secure communications channels 405 - to approve and/or process the financial transaction. The communication with financial networks may also trigger additional or alternate financial processes, such as capture or even refunds. The results of processing by the financial networks 404 will be recorded in the payment server database. The payment
25 server then generates a digital receipt (DR) containing the results of the transaction and sends the receipt to the shop & buy application. The digital receipt contains sufficient information to uniquely identify the customer (by the session identifier, locale and amount), along with the response and authorisation codes supplied by the financial networks. The digital receipt, again encrypted and
30 signed, is sent by re-directing the customer browser to a specific merchant shop & buy application URL, being the return URL supplied in the digital order. Any errors, such as insufficient funds or a communication error, are transmitted to the shop & buy application by the digital receipt.

(9) The merchant shop & buy application on the merchant server uses the payment client to de-encrypt the digital receipt and validate the associated signature. The encryption and digital signature seeks to ensure that the contents of the digital receipt are not tampered with, and that the message is private and can only be decrypted by the intended recipient, ie. the merchant identified in the original digital order. In the embodiment, the digital receipt contains an echo of the order contents to assist in payment matching and several fields returned by the financial networks or added by the merchant server.

(10) The shop & buy application then presents the customer with order confirmation, which uses the contents of the digital receipt, and follows with a "thank you" to complete the electronic shopping event.

It is possible for the financial (payment) transaction to be processed and the merchant's shop & buy application to then fail. The session with the user may be lost as a consequence. However, the checks and balances built into the shop & buy application and the merchant administration facilities enable reconciliation and reconstruction.

For example, if a payment gateway loses connectivity with the customer for whatever reason (eg. customer's modem link failure), the payment server may not be able to deliver the results of a transaction (ie. a digital receipt) if the payment process has progressed that far. However, the payment server expects an acknowledgment for each digital receipt it transmits. If an acknowledgment is not received, the payment server can re-send the DR directly to the merchant's shop & buy application. Before re-sending, the transaction database entry is marked as "undelivered". The re-transmission is attempted a specified number of times with an increasing time delay between retries. If an acknowledgment is received the database transaction record "undelivered" marker is removed. If an acknowledgment is not received, the merchant on subsequent inspection of the database through the merchant administration processes, notes the "undelivered" status and may then cause a new DR to be returned directly to the shop & buy application.

The payment server provides full transactional integrity throughout the payment adapter. Once payment details have been received and validated for correctness by the appropriate payment gateway, a transaction request is initiated and passed to the payment adapter. From this point, transactional integrity is present. A transaction desirably must:

- complete with a financial approval or decline, or a recognizable error,

- be logged in the payment adapter transaction database and
- be passed back to the requesting payment gateway.

If a failure occurs in the processing of a transaction (eg. a communications failure or hardware failure), a persistent store of pending transactions allows rollback of the transaction to a known state. The rollback process depends on the transaction type.
5 Some transaction types require reversing, others require retry until successful completion.

This transactional integrity allows the payment adapter to be regarded as a reference transaction-state portal. By inspecting the payment adapter transaction
10 database, both the merchant and the merchant's bank may reconcile their systems. Merchant shop & buy system reconciliation is achieved by the ability of the payment adapter to "on-demand" re-send undelivered digital receipts to the merchant application.

As with all elements of the payment server of the preferred embodiment, the payment pages presented to the payee are internationalised. In the embodiment, an
15 important element to be passed in the digital order from the payment client is a "locale identifier". This field denotes the language to be used in the presentation of pages to the payee. It should be noted however that this language sensitive locale identifier does not affect the currency to be used. Currency is specified by the merchant. For example, a payee could be presented with pages in Chinese language but using a merchant currency
20 of US dollars.

The payment server may also offer a number of processes to aid in fraud prevention, detection and risk management of both payees and payers. All payment instrument details presented to the payment gateways should pass appropriate fraud prevention checks. These checks include the following:

- 25
- basic card or account number format and consistency checks (eg LUHN or checksum checks);
 - hot-list checking for both individual card and BIN (Bank Identification Number);
 - merchant certificate checking (SET only); and
 - velocity and similar usage pattern checks.
- 30

Merchants may have a variety of risk management controls applied to them by the financial institution. To obviate the requirement to modify bank host systems, the payment server can provide a range of these controls including:

- retained or deferred payments;

- transaction limits within defined rolling periods;
- tools to survey customers on service quality from merchants; and
- on-account payment mechanisms where merchants offer their own “store” credit to customers.

5 A range of heuristic parameters may be applied to these methods to monitor, control and report on merchant risk factors.

In addition to financial transaction processes, the payment server can be used to provide a range of value-added services for merchants or service providers. These value-added services may take several forms depending on the payment server configuration and the financial institution offered services. Various payment instruments, for example
10 smart-cards, provide globally unique identifiers. Typically these tokens are used in conjunction with a secret value known only to the token holder. The secret value may be a PIN (Personal Identification Number) or PCN (Personal Card Number) or a variant of these. The combination of a physical token and the related secret value offers an
15 authentication mechanism.

Additionally, the physical token may hold user information, suitably encrypted, inaccessible without the PIN or PCN. This information may be demographic information, such as name, billing address, account information or it may be electronic identification such as a certificate. The certificate, signed by a trusted authority, contains
20 the user’s public key that may be used to digitally sign authorization messages. Authenticating users can form a value-added service by financial institutions to service providers such as on-line share traders. Supplying certain demographic data, eg. home address, account validation or age verification, can offer significant value to service providers obtaining registration information from customers. The cost reduction in error
25 and fraud handling for these merchants allows the financial institutions to charge fees for these services.

The Payment Server software components are modular and may run as multiple instances. This flexibility can aid scalability and resilience. At one extreme, each component may reside on separate distributed servers; alternatively all components may
30 reside on the one server. For performance scaling and load-balancing and for redundancy purposes, multiple instances of all gateways and the adapter can be provided. Integrity of a common database is achieved through standard disk-mirroring techniques.

The architectural framework of an electronic commerce payment system, including a fully featured payment server, of a second embodiment is illustrated in FIG.

5. This framework provides an extensible, end-to-end, payment systems infrastructure supporting a wide range of current and proposed payment systems for a financial institution or commerce service provider. The framework provides extensibility and flexibility through a family of modular software products that support easy future
5 upgrades and protection against technology obsolescence. The second embodiment includes a series of flexible messaging schemes that provide independence from technology algorithms (eg. cryptographic routines) as well as independence from the attributes of specific payment systems.

In particular, payer segments 501-506, including Internet merchant or hosted
10 ISP/CSP segment 504 (as described in detail above in the first embodiment) are shown in relation to their typical delivery channel/enabling technology 507-512 and the payment server 500 with payment adapter 513, gateways 514, payment registration enabler 516 and bank administration 519. The second embodiment supports both "simple transactions" involving two or three parties (eg. consumer to business and the bank) and
15 "complex transactions" between multiple (N) parties (eg. business to business and their banks). Some examples are:

- single payer to single payee transactions eg. business (electronic) cheque payments through the corporate merchant/buyer segment 505; Typically, these type of transactions, whilst directly transacted between only two parties, actually
20 involve an additional two parties to authorise and settle the transaction - the payer, payee, payee's bank (often called the 'acquirer') and payer's bank (often known as the 'issuer').
- single payer to multiple payees transactions eg. payroll payments, gyro payments involving the retail consumer/account holder segment 506;
- 25 • multiple payers to a single payee transactions eg. batched MOTO (Mail Order, Telephone Order) payments for merchant segment 502;
- multiple payers to multiple payees transactions eg. EDI payments, ACH (Automated Clearing House) settlements; and
- hybrid combinations of the above, eg. recurring payments involving 2-
30 party & multi-party payers and payees.

The architectural framework of the system, not only supports the direct parties conducting the payment transactions, but also supports the financial institutions 520 (the acquiring and issuing institutions) whom provide the infrastructure to support the

authorization and settlement functions between 2-party, 3-party and N-party transactions described above.

5 The system of the second embodiment may be supported on a range of operating system platforms. Cross-platform support is provided through use of Java as the major programming language. The system supports industry-standard technology platforms for payers and payees such as Internet browser platforms using well known protocols such as HTTP, HTTPS (Secure HTTP) and portable data description standards such as HTML and XML (eXtensible Markup Language).

10 The system includes a common module, called the payment adapter 513, through which all transactions are managed, communicated, logged in a database. The payment adapter is responsible for transaction and system integrity. A single payment adapter will support one or multiple payment gateways 514 or multiple instances of a single type of payment gateway. The payment adapter may be configured itself with multiple instances. The architecture is inherently scalable across multiple processors or distributed machines.

15 The payment adapter provides ease of installation to financial institutions by supporting known financial protocol standards 515 (eg. ISO8583, AS2805, APACS) and through rapid integration with bank authorization and settlement systems through use of flexible message-mapping toolsets.

20 The system supports an extensible family of plug-and-play payment gateways to manage specific types of payment transactions. This family of gateways means a financial institution can easily upgrade from one payment scheme to another, as and when required. All Payment Gateways communicate with and are supported by the common Payment Adapter.

25 The System Architectural Framework provides software technology to enable payers and payees to conduct secure, authenticated transactions through an extensible family of payment clients. The payment gateways, together with the payment clients provide the fundamental transaction co-ordination between the financial institution and their customer, whether they are payer or payee.

30 The system of the second embodiment provides a means to implement and manage version control of payee software. It provides dynamic upgrade support for new payment schemes for payees (eg. merchants) without upgrading the payment client software on the payees computer systems. This upgradability is achieved through a combination of payment instrument-independent payment clients and through

dynamically served server-side templates or applets. These server-side templates or applets can be modified at any time under the control of the financial institution and then enabled for subsequent transactions. This ability to upgrade enables banks to offer new services to merchant customers rapidly and at low cost.

5 Payment clients, in conjunction with other components of the payment system, the payment adapter 513 and one or more payment gateways 514, are operative to provide bi-directional authenticated transaction management and communication to and from the particular payment gateway. Authentication of the identity of the payer or payee is provided through one or more public and private key techniques, along with
10 additional authentication tokens such as secure user-IDs, passwords, digital certificates PINs (Personal Identification Numbers), etc.

 The payment system architecture provides an automated Internet-based means to centrally register payers or payees and to distribute enabling software technology over the Internet to the banks customers, whether they be payers or payees. This logistical
15 management tool is the Payment Registration Enabler (PRE). The PRE performs the role of generating unique payment clients for each registered user, through the creation of unique cryptographic key pairs embedded in the enabling software. PRE lowers the cost of installing, maintaining and upgrading payer and payee customers of the bank as it performs these functions without human intervention through an automated web-based
20 software application.

 In any practical real-world payment system, a specific configuration of these architectural elements combine to ensure that the payment system is trusted and works effectively to protect all parties involved in financial payment transactions. By abstracting these core elements into an architectural design, the system of the second
25 embodiment provides an architecture that is both flexible and future-proof. Examples of the most-common payment protocols or systems used today in the financial community which the payment system can support include:

 □ On-line, real-time card payment protocols eg. ISO8583/AS2805. Whether the card payment scheme is one designed to support pay before (eg. stored value
30 on a card, other token or system), pay now (debit) or pay later (credit). These types of low and medium value payment systems are typically supported by banks and the major card associations such as Visa, MasterCard and American Express.

 □ On-line real-time non-card payment systems, eg. RTGS. These types of

payment systems generally authorise and settle high-value transactions between participating entities.

- 5 □ Offline batch payment systems eg. electronic cheque payments, mail order/ telephone payments. These types of payment systems are typically run by clearing houses that settle between participating entities on a periodic basis. Examples of such systems include ACH in the USA, BACS in the UK, BECS in Australia.
- 10 □ Cash-type payment systems for example e-cash & stored value systems. These payment systems emulate real cash and support real-time monetary transfer at the time of payment.
- Other payment systems for example micro-payments and payments over specialized device networks (eg. phone, Internet PC).

In most applications the payment server, which centrally hosts the PRE 516, the gateway modules 514 and the payment adapter 513 connects directly to the payee bank, typically the acquiring merchant's bank (Acquirer), via the financial networks 520. In the case of the transaction containing NOT-ON-US payment instruments, eg credit cards not issued by the acquiring bank, the payment needs to be authorized by the issuer of the payment instrument. In some cases this messaging to the issuer is done by internal Acquiring bank systems. This is the typical 3-party transaction. In some cases the Payment Server is used to message directly to the Issuer Bank (or Issuer's proxy). In this case, the transaction becomes a 4-party transaction.

The systems architecture of the second embodiment can support N-Party transaction where, effectively, multiple transactions are generated from one initiating transaction. There are several examples of such processing, wherein a system configured in accordance with the second embodiment may form the nucleus of a trading hub for Business to Business (B2B) transactions. A single shopping purchase from one of a group of electronically linked businesses may trigger a chain of related transactions such as shipping or payment of taxes. An example of the operation of a trading hub 600 is now described with reference to FIG. 6.

30 A customer shops on-line, using their computer system 601, at the on-line shopfront of merchant #1, namely the shop & buy server 611. The customer selects goods and proceeds to the payment process, as described previously in relation to FIG. 2. A transaction similar to a 3-party process begins, except that the digital order contains additional information. This Extended Digital Order (EDO) contains information that

will allow further transactions in a fulfilment chain to be automatically triggered.

If the initial transaction is successful, a Digital Receipt is returned to merchant server 611 by a payment server 630 as per normal and the following transactions may be automatically triggered:

5 A delivery request is made to a shipper (eg. FedEx) with a payment and with details of the shipping cost. The details of the shipper, the shipping cost, and related shipping information (air freight, destination city) are built into a second digital receipt (DR #2) generated automatically by the payment server 630. This second digital receipt is transmitted to the shipper's ERP system 620, here merchant #2. Merchant #2 then
10 processes the DR #2 and returns an acknowledgment to the payment server 630 (part of payment client functionality). Merchant #2 would act upon the information as per their contract with merchant #1. Simultaneously, a transaction is generated by the payment server to the payee (merchant #2) account with merchant #1 as the payer.

 A second example of an automatically triggered transaction is the payment of
15 taxes, eg. goods and services tax (GST), at the time of the transaction. The taxation office would be merchant #3 (not shown) also interfaced to the payment server 630 in that example, by a suitable payment client. Thus multiple automatically triggered transactions can be supported.

 The benefits which flow from the embodiments of the invention include the
20 following:

- (i) security of transmission – the PKI messaging ensures that only the intended parties may decrypt the contents of transmitted messages;
- (ii) authentication of sender – the PKI digital signatures guarantees that the message has originated from the specified payee;
- 25 (iii) integrity of data - the PKI digital signatures guarantees that the message has not been corrupted, either maliciously or accidentally, during transmission;
- (iv) protection of the payment details (eg. credit card number) – the payment details are provided directly to the payment server by the payer for communication only with financial networks, merchant fraud or unauthorised re-use is largely obviated;
- 30 (v) simple payee integration – a wide range of payment protocols are implemented at the payment server;
- (vi) improved control of payee options and actions – financial institutions or operator of the payment server decides payee privileges and permissible payment instruments; and

(vii) ease of change or updating available payment options - may be added by the payment server without requiring the payee to modify any application.

5 Although illustrative embodiments of the present invention, and various modifications thereof, have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to these precise embodiments and the described modifications, and that various changes and further modifications may be effected therein by one skilled in the art without departing from the scope or spirit of the invention as defined in the appended claims.

CLAIMS

1. A payment method for electronic commerce involving a payer computer, a payee computer and a payment gateway, said method including the steps of:

5 (a) the payee computer creating, in response to transmission of a payment request from the payer computer over a communications link to said payee computer, a transaction order containing a transaction amount, a transaction identifier and a payee identifier;

10 (b) the payee computer transmitting the transaction order to the payment gateway over a secure communications link, and linking the payer computer to the payment gateway;

(c) the payment gateway validating the transaction order, obtaining payment details associated with the transaction request from the payer computer, and forwarding the transaction amount and payment details to a financial network for further processing;

15 (d) the payment gateway producing a transaction receipt in response to said further processing by the financial network, transmitting the receipt to the payee computer, and re-linking the payer computer to the payee computer; and

(e) the payee computer transmitting transaction status information contained in the transaction receipt to the payer computer.

20

2. The payment method of claim 1 wherein both the transaction order and the transaction receipt are digitally signed and encrypted in order to facilitate authentication of the transmitting party and to protect the integrity of the respective contents of the transaction order and receipt.

25

3. The payment method of either claim 1 or claim 2 wherein the transaction request from the payer computer is transmitted over a secure communications link.

30 4. The payment method of any preceding claim wherein the transaction request includes the transaction amount and the transaction identifier.

5. The payment method of any preceding claim wherein the transaction request contains details of items to be purchased.

6. The payment method of any preceding claim wherein the processing by the financial network involves authorisation of payment that occurs in real time.

5 7. A payment apparatus for effecting payment transactions in electronic commerce, said payment apparatus including:

(a) a payee computer operative to receive a transaction request from a payer computer over a communications link and creating, in response to the transaction request, a transaction order containing a transaction amount, a transaction identifier and a payee
10 identifier;

(b) the payee computer also operative to transmit the transaction order to a payment gateway over a secure communications link, and to effect linking of the payer computer to a payment gateway;

(c) the payment gateway operative, subsequent to validating the transaction
15 order, to obtain payment details associated with the transaction request from the payer computer and to forward the transaction amount and payment details to a financial network for further processing;

(d) the payment gateway also operative to produce a transaction receipt in response to said further processing by the financial network, to transmit the receipt to the
20 payee computer, and to effect re-linking of the payer computer to the payee computer; and

(e) the payee computer then operative to transmit transaction status information contained in the transaction receipt to the payer computer.

25 8. The payment apparatus of claim 1 wherein a payment client application is resident on the payee computer to facilitate secure communications with the payment gateway.

9. The payment apparatus of either claim 1 or claim 2 wherein the payment
30 gateway is one of a plurality of such gateways hosted on a payment server, which payment server also hosts a payment registration enabler application and a payment adapter application.

10. The payment apparatus of claim 9 wherein the payment registration enabler application generates unique identifiers for payment clients registered with the payment server.

5

11. The payment apparatus of claim 9 wherein the payment adapter application provides an interface between the respective gateways and financial networks.

10

12. A method of conducting electronic transactions involving a customer for goods or services supplied by a merchant, wherein a customer browser and a merchant server can communicate with each other and with a payment server, and the payment server can communicate separately with a plurality of financial institutions, said method including the steps of:

15 (a) the customer browser transmitting a payment request for one or more items desired to be purchased by the customer to the merchant server;

(b) the merchant server providing in response to the payment request a merchant identifier, transmitting the merchant identifier together with a session identifier and payment amount required for the desired items over a secure communications link to the payment server, and redirecting the customer browser to the payment server;

20

(c) the payment server validating the merchant identifier and requesting payment information from the customer, then using the session identifier and the payment information to seek approval for payment from the customer's financial institution;

25 (d) the payment server providing a receipt regarding the approval to the merchant server over the secure communications link and redirecting the customer browser to the merchant server; and

(e) the merchant server providing approval status information about the transaction for purchase of the items to the customer browser.

30

13. The method of claim 12 wherein step (a) involves the customer perusing electronic catalogues and adding items of goods or services to a virtual shopping basket of a shop and buy application executing on the merchant server, in order to identify the desired items.

14. The method of either claim 12 or claim 13 wherein, in step (a), delivery information obtained from the customer is transmitted to the merchant server.

5 15. The method of any one of claims 12 to 14 wherein, in step (b), the merchant server executes a payment client application that creates a digital order containing the merchant identifier, session identifier and payment amount, which digital order is transmitted to the payment server.

10 16. The method of any one of claims 12 to 15 wherein, in step (c), the payment information includes payment method, in the form of payment protocol and payment instrument, and payment details.

15 17. The method of claim 15 wherein the digital order further contains a locale identifier denoting the language to be used in presentations to the customer by the payment server and a return universal resource locator (URL) which enables the payment server to route a digital receipt to the merchant server or associated merchant application.

18. The method of claim 15 wherein the digital order is secured and
20 authenticable by means of a merchant key pair recognisable by the payment server.

19. The method of claim 15 wherein the digital order includes encryption of the information contained along with a digital signature to effect authentication and message integrity.

25 20. The method of claim 12 wherein step (d) further involves the merchant server acknowledging receipt of the digital receipt to the payment server.

30 21. The method of claim 20 wherein, in the absence of the acknowledgment of the digital receipt from merchant server the transaction is flagged as undelivered, and the payment server re-sends the digital receipt to the merchant server.

22. An electronic transaction apparatus for use in conjunction with a merchant server hosting a shop & buy application allowing a customer to peruse, via a communications link with a customer computer, goods and services supplied by the merchant, said apparatus including:

(a) a plurality of payment clients for integration with the shop and buy application on the merchant server, said payment clients facilitating secure communications with a payment server using respective payment protocols;

(b) a payment server having a plurality of payment gateways corresponding to at least one of the payment clients of the merchant server, and a payment adapter providing an interface for separate communications with a plurality of financial institutions; and

(d) the payment server operative to process customer payment orders produced by a payment client in response to the shop and buy application and transmitted by the merchant server; whereby, in use:

(i) the customer computer is redirected to the payment server to obtain payment details from said customer in order to seek approval from the customer's financial institution, and

(ii) the payment server provides a receipt to the merchant server regarding the approval before redirecting the customer computer back to the merchant server.

23. The transaction apparatus of claim 22 wherein the shop and buy application is an Internet storefront accessible by a browser application resident on the customer computer.

24. The transaction apparatus of either claim 22 or claim 23 wherein the payment clients are implemented using active code for execution by a virtual machine emulator resident on the merchant server.

25. The transaction apparatus of any one of claims 22 to 24 wherein the payment server provides a secure communications link between the payment server and the customer.

26. The transaction apparatus of any one of claims 22 to 25 wherein the customer order is a digital order containing a merchant identifier, a session identifier and a payment amount required by the merchant for purchase of items desired by the customer.

5

27. The transaction apparatus of any one of claims 22 to 26 wherein the payment server includes a transaction database for recording details of payment transactions for merchants.

10

28. The transaction apparatus of any one of claims 22 to 27 wherein the merchant receipt is preferably a digital receipt containing an authorisation code for the customer.

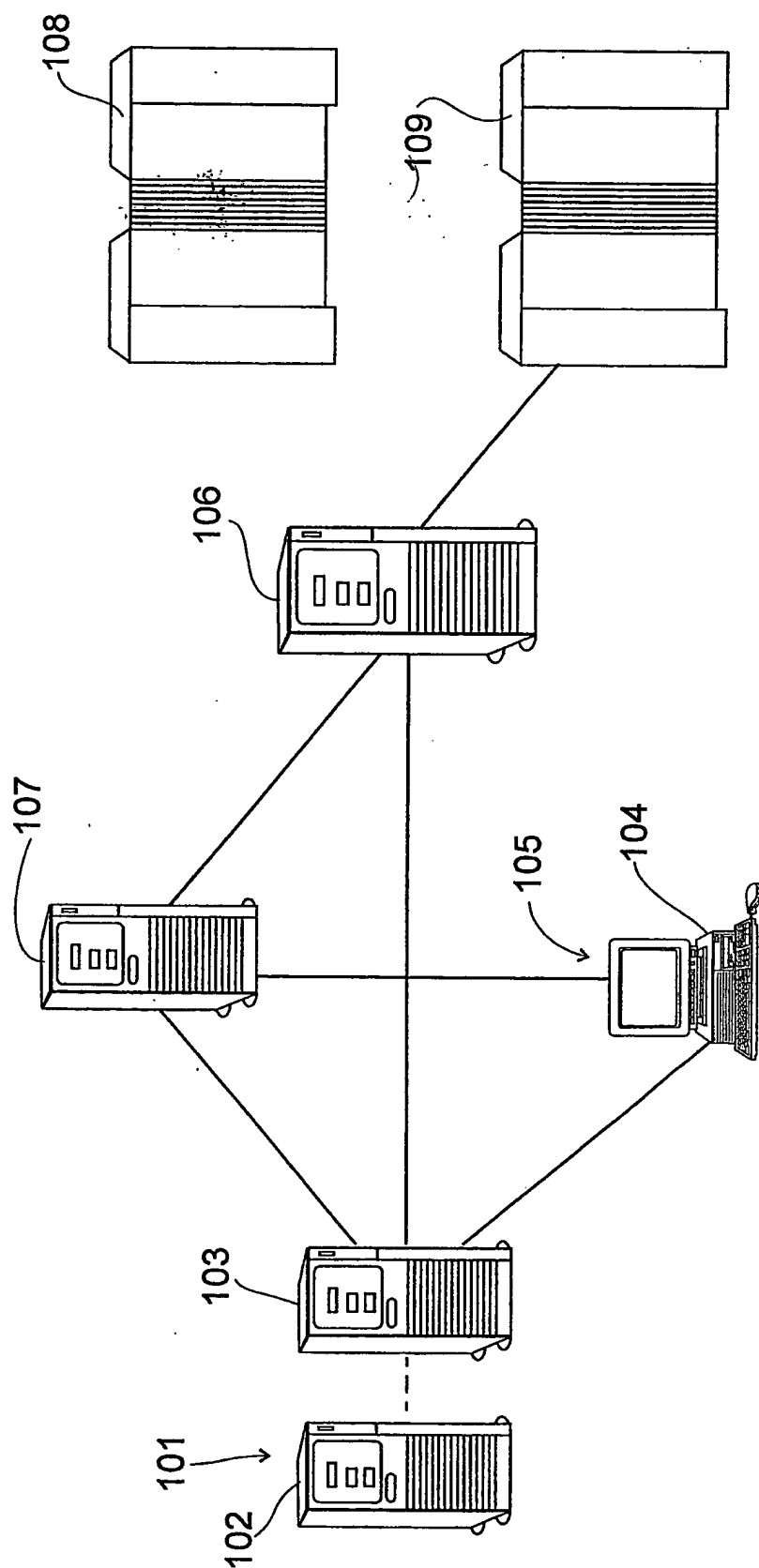
15

29. The transaction apparatus of any one of claims 22 to 28 wherein the payment server further includes a payment registration application that generates and distributes pairs of security keys to respective payment clients.

30. The transaction apparatus of claim 27 wherein both the digital order and the digital receipt are encrypted and digitally signed using the security key pairs.

20

1 / 7



Prior Art

FIG. 1

2 / 7

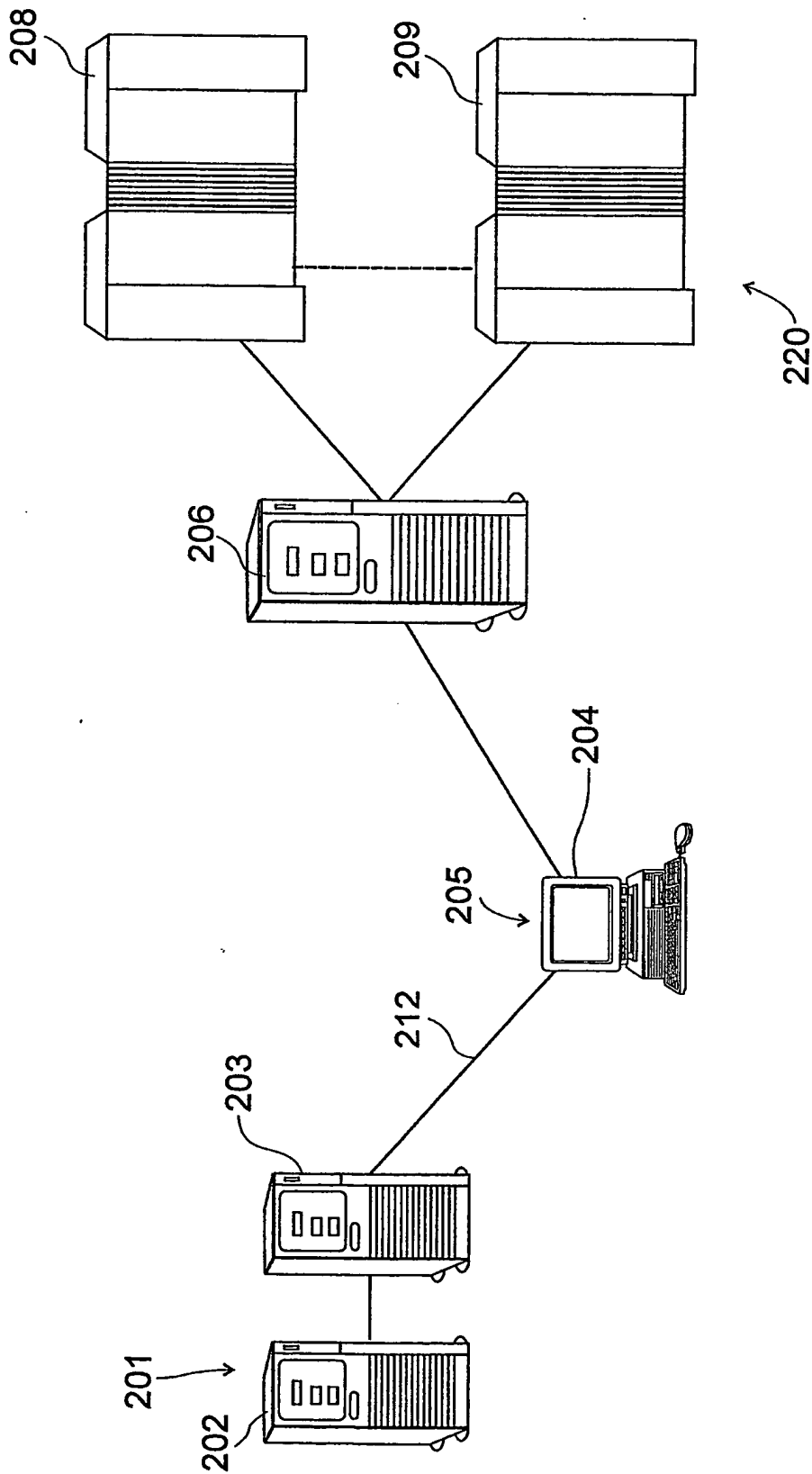


FIG. 2

3 / 7

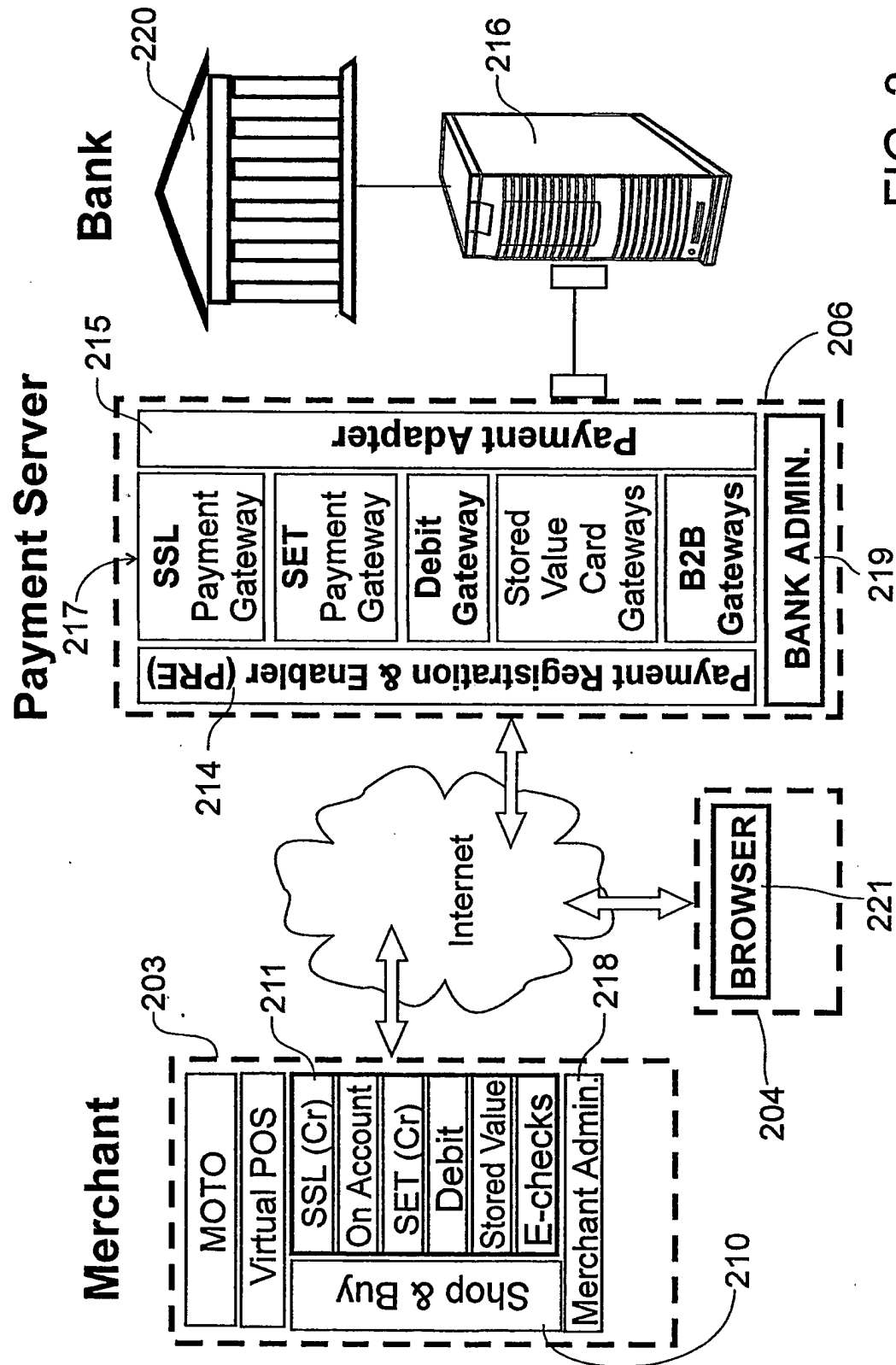


FIG. 3

4 / 7

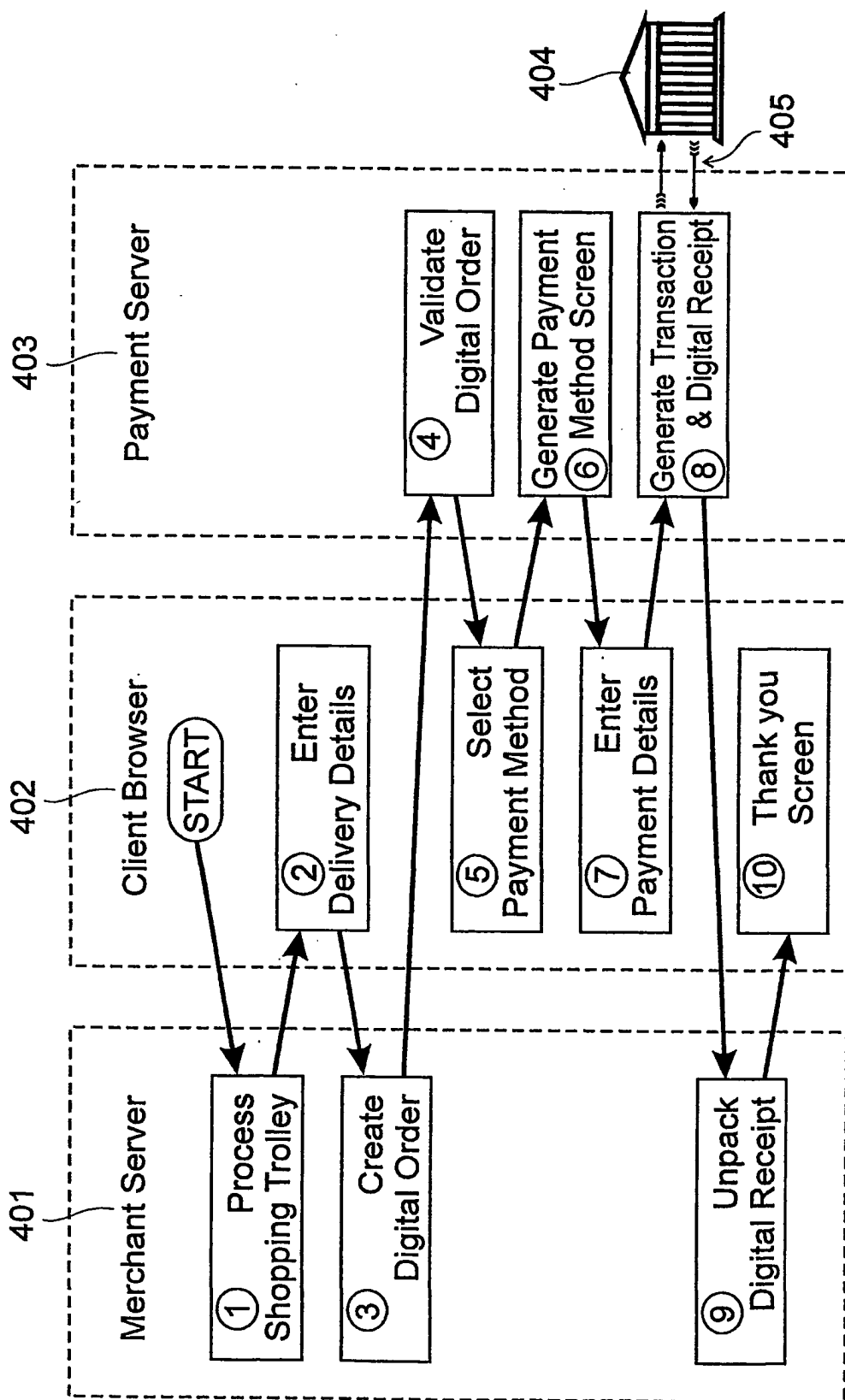


FIG. 4

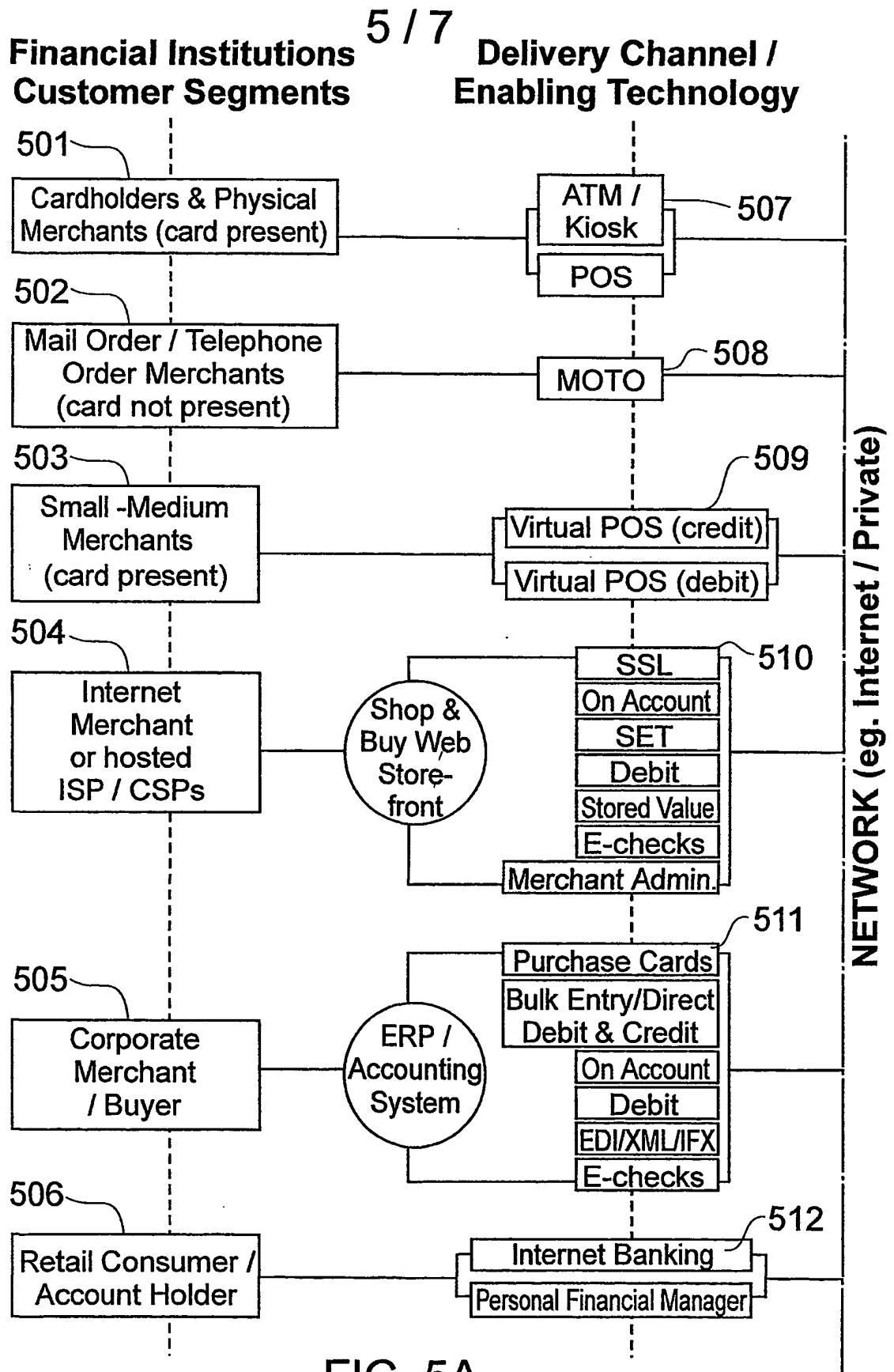


FIG. 5A

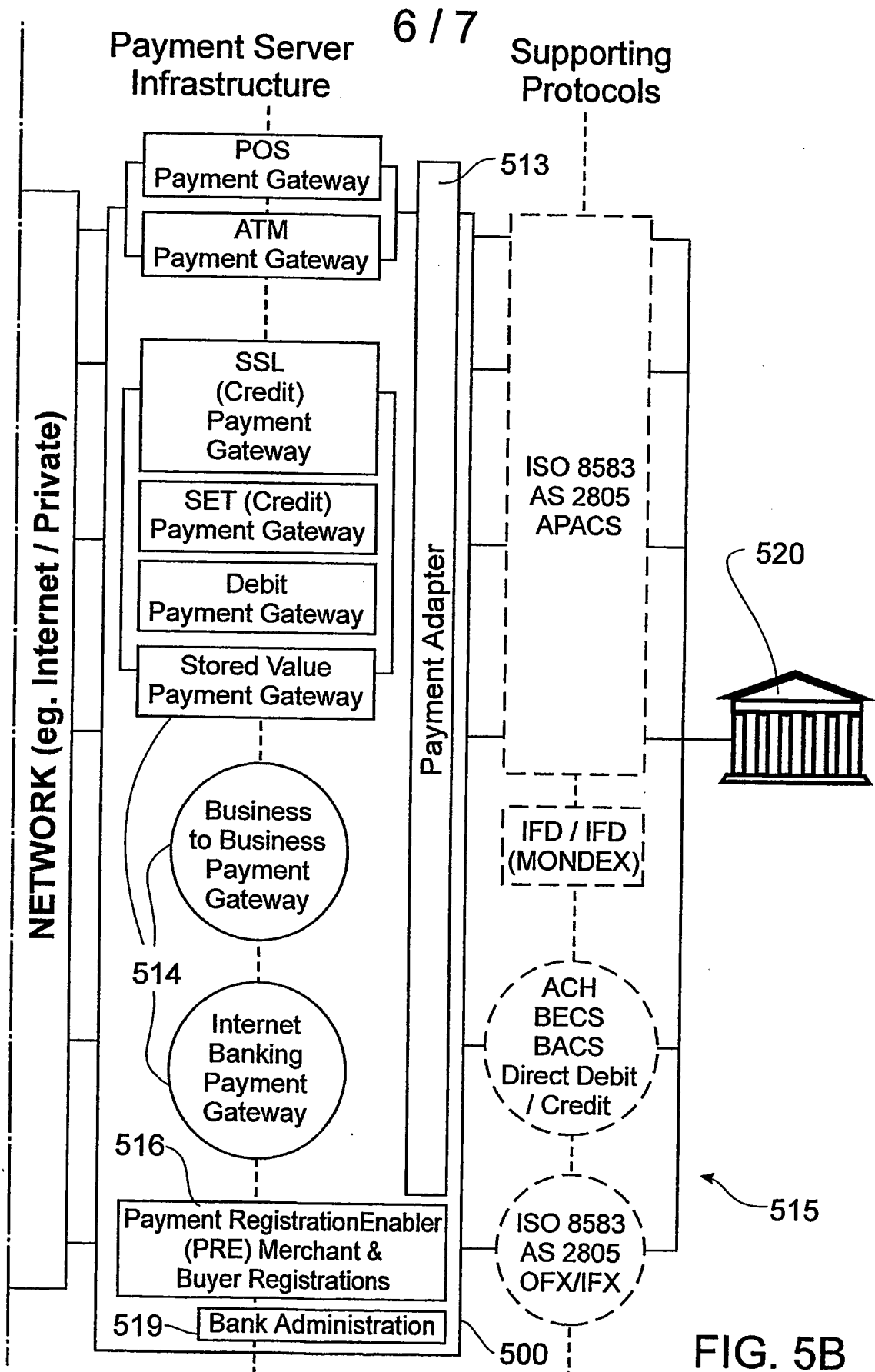


FIG. 5B

7 / 7

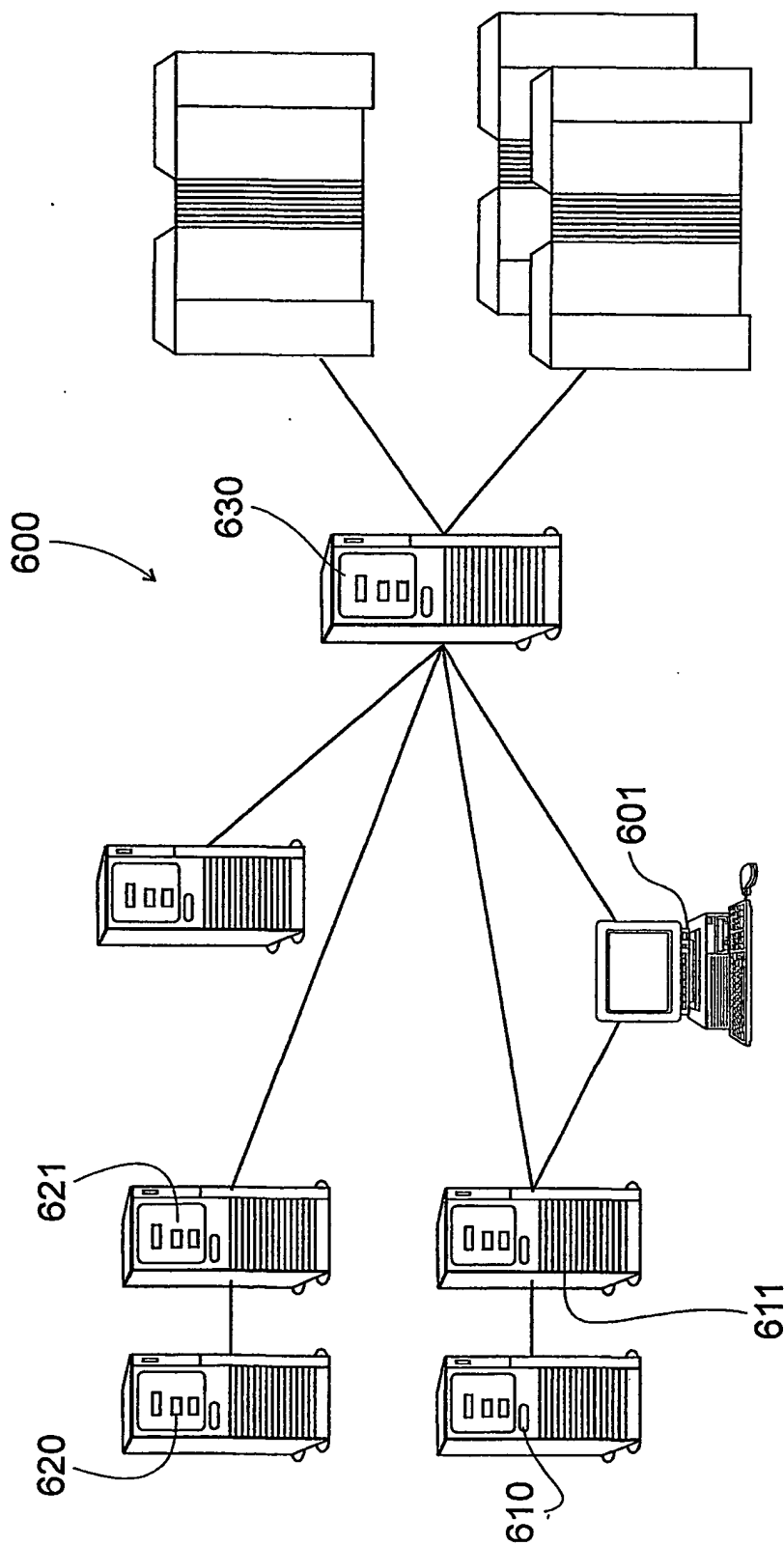



FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU01/00430

A. CLASSIFICATION OF SUBJECT MATTER												
Int. Cl. ⁷ : G06F 17/60												
According to International Patent Classification (IPC) or to both national classification and IPC												
B. FIELDS SEARCHED												
Minimum documentation searched (classification system followed by classification symbols)												
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched												
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT, USPTO (KEYWORDS)												
C. DOCUMENTS CONSIDERED TO BE RELEVANT												
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.										
X	WO, A, 99/07121 (NETADVANTAGE CORPORATION) 11 February 1998 - see whole document	1-30										
<input type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex												
<p>* Special categories of cited documents:</p> <table border="0"> <tr> <td>"A" document defining the general state of the art which is not considered to be of particular relevance</td> <td>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</td> </tr> <tr> <td>"E" earlier application or patent but published on or after the international filing date</td> <td>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</td> </tr> <tr> <td>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</td> <td>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</td> </tr> <tr> <td>"O" document referring to an oral disclosure, use, exhibition or other means</td> <td>"&" document member of the same patent family</td> </tr> <tr> <td>"P" document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </table>			"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family	"P" document published prior to the international filing date but later than the priority date claimed	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention											
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone											
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art											
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family											
"P" document published prior to the international filing date but later than the priority date claimed												
Date of the actual completion of the international search 25 May 2001		Date of mailing of the international search report 01 JUN 2001										
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. (02) 6285 3929		Authorized officer  Stephen Lee Telephone No : (02) 6283 2205										

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/00430

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
WO	9907121	AU	86753/98	EP	1004086
END OF ANNEX					